EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

18 mai 2022

Avis 9/2022

sur la recommandation de décision du Conseil autorisant les négociations en vue d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

edps.europa.eu

Le Contrôleur européen de la protection des données (le «CEPD») est une institution indépendante de l'Union chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union», et en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Rafał Wiewiórowski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

*En vertu de l'**article 42, paragraphe 1**, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».*

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'Union européenne sur l'application cohérente et logique des principes de protection des données de l'Union européenne, notamment lors de la négociation d'accords avec des pays tiers dans le secteur de l'application de la loi. Il s'appuie sur l'obligation générale exigeant que les accords internationaux soient conformes aux dispositions du traité sur le fonctionnement de l'Union européenne («TFUE») et respectent les droits fondamentaux qui forment le noyau du droit de l'Union. En particulier, il convient de veiller au respect des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne ainsi que de l'article 16 du TFUE.

Le présent avis n'exclut pas que le CEPD formule ultérieurement des observations ou des recommandations supplémentaires, en particulier si d'autres problèmes sont détectés ou si de nouvelles informations apparaissent. En outre, le présent avis est sans préjudice de toute mesure future qui pourrait être prise par le CEPD dans l'exercice des pouvoirs qui lui sont conférés par le règlement (UE) 2018/1725. Le présent avis se concentre sur les dispositions pertinentes de la recommandation en matière de protection des données.

Synthèse

Le 29 mars 2022, la Commission européenne a publié une recommandation de décision du Conseil l'autorisant à participer, au nom de l'Union européenne, aux négociations que les Nations unies mènent en vue d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Le CEPD comprend que les services répressifs doivent pouvoir recueillir et obtenir des preuves électroniques rapidement et efficacement. Il souligne toutefois qu'un instrument international similaire est déjà en vigueur, à savoir la convention sur la cybercriminalité et son deuxième protocole additionnel, à présent ouvert à la signature.

Le CEPD fait observer que les Nations unies ont déjà entamé des négociations en vue d'une autre convention visant à traiter les questions de la cybercriminalité et de la coopération transfrontière en matière pénale. Il approuve donc la recommandation autorisant la Commission à participer aux négociations au nom de l'Union, étant donné que cela contribuerait à préserver le niveau de protection que garantit le cadre de l'Union en matière de protection des données. Le CEPD constate toutefois que les Nations unies comptent de nombreux pays, lesquels disposent de systèmes juridiques extrêmement hétérogènes. Dans ce contexte, il estime qu'il existe un risque important que la version définitive de la convention puisse entraîner une réduction des libertés et droits fondamentaux dont les personnes physiques jouissent en vertu du droit de l'Union, notamment leurs droits à la protection des données et au respect de la vie privée. Par conséquent, force est de souligner que dans l'éventualité où le Conseil autoriserait la Commission à négocier dans ce cadre au nom de l'Union, cette autorisation n'obligerait pas cette dernière à devenir partie à la convention en cas d'adoption. Le CEPD estime que l'Union ne devrait pas chercher à être partie à une telle convention si le niveau de protection des données que le droit de l'Union garantit aux personnes physiques devait diminuer.

Le présent avis vise à fournir des conseils constructifs et objectifs aux institutions de l'Union de façon à ce que le niveau de protection des données garanti par le droit de l'Union ne soit pas compromis. Le CEPD se félicite du fait que le mandat vise à garantir d'emblée que la convention prévoit des conditions strictes et des garanties solides afin que les États membres de l'Union puissent respecter et protéger les droits fondamentaux, les libertés et les principes généraux du droit de l'Union, tels qu'ils sont consacrés dans les traités européens et la Charte.

Dans ce contexte, le CEPD souligné la nécessité de garantir, notamment, le respect absolu des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. Le régime juridique de l'Union en matière de protection des données prévoit, en principe, que les transferts de données vers un pays tiers ne peuvent avoir lieu sans exigences supplémentaires que si ce pays tiers garantit un niveau de protection adéquat. Lorsque le pays tiers n'a pas été déclaré adéquat, des exceptions s'appliquent à certains transferts, jusqu'à ce que les garanties appropriées soient apportées. Même si le CEPD reconnaît qu'il peut être impossible de transposer la terminologie et les définitions du droit de l'Union dans un accord avec de nombreux pays tiers, il insiste sur le fait que les garanties des particuliers doivent être claires et efficaces afin de pleinement respecter le droit de l'Union. Ces dernières années, la Cour de justice de l'Union européenne a de nouveau confirmé les principes relatifs à la protection des données, y compris le

droit à un recours juridictionnel et les droits individuels des personnes. Ces principes s'avèrent d'autant plus importants que les données nécessaires aux enquêtes pénales sont sensibles.

Dans ce contexte, le CEPD considère que, si nombre de directives de négociation déjà envisagées sont accueillies favorablement, elles devraient être renforcées. Plus précisément, dans le but de garantir le respect de la Charte et de l'article 16 du TFUE, le CEPD formule quatre recommandations essentielles concernant les directives de négociation:

- limiter les dispositions en matière coopération internationale aux infractions pénales définies dans la convention;

- exclure l'accès direct des services répressifs de pays tiers aux données et la coopération transfrontière directe avec des fournisseurs de services;

- veiller à ce que les futurs accords bilatéraux et multilatéraux conclus avec des pays tiers s'appliquent en lieu et place de la convention s'ils garantissent des normes plus élevées en matière de protection des droits fondamentaux, notamment des droits au respect de la vie privée et à la protection des données;

- veiller à ce que la convention ne produise aucun effet entre deux États contractants si l'un d'entre eux notifie le fait que la ratification, l'acceptation, l'approbation ou l'adhésion d'un autre État contractant n'aura pas pour effet d'établir des relations entre ces deux États contractants en vertu de ladite convention.

En outre, l'avis contient des recommandations supplémentaires relatives à des améliorations et des éclaircissements à apporter aux directives de négociation. Les observations présentées dans le présent avis sont sans préjudice des observations supplémentaires que le CEPD pourrait formuler ultérieurement, notamment si de nouveaux problèmes étaient soulevés et abordés à la lumière d'informations complémentaires. Le CEPD s'attend à être consulté ultérieurement à propos des dispositions du projet de convention avant que celui-ci ne soit finalisé.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données[1] («RPDUE»), et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. L'Organisation des Nations Unies est une organisation internationale, qui compte aujourd'hui 193 États membres[2]. La mission et le travail des Nations unies sont guidés par les objectifs et principes énoncés par sa charte fondatrice. Conformément à la charte des Nations unies, l'organisation a notamment pour but de maintenir la paix et la sécurité internationales, de défendre les droits de l'homme, d'apporter une aide humanitaire, de favoriser le développement durable et de veiller au respect du droit international[3].

2. Le 17 décembre 2018, l'Assemblée générale des Nations unies a adopté la résolution 73/187 intitulée «Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles»[4]. Ultérieurement, le 27 décembre 2019, elle a adopté la résolution 74/247[5], en vertu de laquelle elle a décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée (le «comité spécial») ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Elle y souligne qu'il faut renforcer la coordination et la coopération entre les États dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, notamment en fournissant aux pays en développement qui en font la demande une assistance technique. La résolution met également en évidence la nécessité d'améliorer la législation et les cadres nationaux et de renforcer les capacités des autorités nationales afin de lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles sous toutes ses formes, y compris de la prévenir, d'en détecter les manifestations, d'enquêter sur celles-ci et d'en poursuivre les auteurs[6], **compte étant pleinement tenu des instruments internationaux existants et des initiatives déjà prises en la matière aux niveaux national, régional et international**, notamment les travaux menés par le groupe intergouvernemental d'experts à composition non limitée chargé d'effectuer une étude approfondie sur la cybercriminalité et les résultats obtenus

[1] *JO L 295 du 21.11.2018, p. 39.*
[2] *Voir la liste des États membres ici: https://www.un.org/en/about-us/member-states*
[3] *Voir le préambule de la charte des Nations unies, San Francisco, 26 juin 1945: https://www.un.org/en/about-us/un-charter/full-text*
[4] *Résolution de l'Assemblée générale des Nations unies du 17 décembre 2018, A/RES/73/187.*
[5] *Résolution de l'Assemblée générale des Nations unies du 27 décembre 2019, A/RES/74/247.*
[6] *Voir la page 1 de la résolution.*

par celui-ci[7]. Trois États membres de l'Union (Estonie, Pologne et Portugal) assurent la coprésidence du comité spécial[8].

3. Le 26 mai 2021, par la résolution 75/282[9], l'Assemblée générale des Nations unies a en outre réaffirmé que le comité spécial **tiendra pleinement compte des instruments internationaux existants** et des initiatives prises aux niveaux national, régional et international pour lutter contre l'utilisation des technologiques de l'information et des communications à des fins criminelles[10]. Elle a décidé que le comité spécial tiendra au moins six sessions et conclura ses travaux de manière à lui présenter un projet de convention à sa 78e session, qui devrait débuter en septembre 2023 et se terminer en septembre 2024.

4. La première session de négociation s'est tenue du 28 février au 11 mars 2022. À cette occasion, les objectifs, le champ d'application, la structure et les éléments essentiels de la convention ont été étudiés[11]. D'après le projet de rapport de cette première session de négociation, il a été convenu que les éléments suivants constitueraient la structure de la convention[12]:

   Préambule

   1. Dispositions générales
   2. Incrimination
   3. Mesures procédurales, détection et répression
   4. Coopération internationale
   5. Assistance technique, dont échange de données d'expérience
   6. Mesures préventives
   7. Mécanisme d'application
   8. Dispositions finales

5. La Commission européenne a participé aux réunions du comité spécial en tant qu'observateur. Une consultation intersessions a eu lieu les 24 et 25 mars 2022 pour solliciter les contributions de diverses parties prenantes concernant l'élaboration du projet de convention[13]. La prochaine session de négociation devrait commencer le 30 mai 2022[14].

6. Le 29 mars 2022, la Commission européenne a publié une recommandation de décision du Conseil l'autorisant à participer, au nom de l'Union européenne, aux négociations que les Nations unies mènent en vue d'une convention internationale générale sur la lutte contre

---

[7] Le groupe intergouvernemental d'experts à composition non limitée chargé d'effectuer une étude approfondie sur la cybercriminalité a été créé par la Commission pour la prévention du crime et la justice pénale (CPCJP), établie à Vienne, à la demande de l'Assemblée générale des Nations unies dans sa résolution 65/230. Il s'agit d'un organe subsidiaire de la CPCJP. Ce groupe d'experts est distinct du comité spécial chargé de négocier la convention, lequel est un organe subsidiaire de l'Assemblée générale et est chargé d'une mission différente.

[8] Le comité spécial se compose des membres suivants: Algérie (présidence), Égypte, Nigeria, Chine, Japon, Estonie, Pologne, Russie, République dominicaine, Nicaragua, Brésil, Australie, Portugal, États-Unis (vice-présidence), Indonésie (rapporteure).

[9] Résolution de l'Assemblée générale des Nations unies du 26 mai 2021, A/RES/75/282.

[10] Voir le point 11 de la résolution.

[11] Les commentaires communiqués lors de cette première session sont disponibles ici: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

[12] https://documents-dds-ny.un.org/doc/UNDOC/LTD/V22/012/09/PDF/V2201209.pdf?OpenElement.

[13] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/1st-intersessional-consultation.

[14] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

l'utilisation des technologies de l'information et des communications à des fins criminelles (la «recommandation»)[15]. La recommandation s'accompagne d'une annexe (l'«annexe»), dans laquelle figurent les propositions de directives du Conseil destinées à négocier la convention.

7. La Commission recommande l'adoption d'une décision du Conseil conformément à la procédure établie à l'article 218 du TFUE relativement aux accords conclus entre l'Union et les pays tiers. Par cette recommandation, la Commission cherche à obtenir l'autorisation du Conseil pour être désignée négociateur en chef au nom de l'Union dans le but de garantir la participation appropriée de cette dernière aux négociations avec les Nations unies, lesquelles devraient porter sur des éléments qui concernent sa législation et ses compétences, notamment dans le domaine de la cybercriminalité[16].

8. Le présent avis du CEPD est émis en réponse à une demande de consultation présentée par la Commission européenne le 29 mars 2022, conformément à l'article 42, paragraphe 1, du RPDUE. Le CEPD se félicite de la référence faite à cette consultation au considérant 5 de la recommandation.

2. Propos introductifs

9. D'après l'exposé des motifs, les négociations relatives à la convention devraient porter sur les règles communes de l'Union visant à lutter contre la cybercriminalité. Parmi ces règles pourraient figurer notamment la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, la directive 2013/40/UE relative aux attaques contre les systèmes d'information, et la directive (UE) 2019/713 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[17]. D'autres instruments de l'Union prévoient des règles communes visant à lutter contre des infractions, telles que le terrorisme, la traite des êtres humains, le trafic de drogues, le trafic illicite d'armes, le blanchiment de capitaux, la corruption et la criminalité organisée, qui sont susceptibles d'être facilitées par le recours à des systèmes d'information[18]. Les négociations devraient également porter sur des mesures de procédure pénale et de coopération. L'Union a adopté plusieurs instruments dans ce domaine[19].

10. Le CEPD fait observer que les Nations unies ont déjà entamé les négociations conformément aux résolutions citées ci-dessus, à savoir les résolutions 74/247 et 75/282 de l'Assemblée générale des Nations unies. Compte tenu de l'importance que ces négociations revêtent pour la stratégie de l'Union en matière de cybercriminalité et d'obtention de preuves électroniques en matière pénale, notamment pour la protection de la vie privée et des données à caractère personnel, le CEPD **plaide en faveur de l'adoption d'une**

---

[15] Recommandation de décision du Conseil autorisant les négociations en vue d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles [COM(2022) 132 final]
[16] Voir l'exposé des motifs, p. 2, et l'article 1er de la recommandation.
[17] Voir l'exposé des motifs, p. 3.
[18] Idem.
[19] Idem, p. 4.

décision du Conseil conférant un mandat clair à la Commission européenne pour participer à ces négociations au nom de l'Union.

11. Comme souligné dans la recommandation[20], une nouvelle convention internationale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles est susceptible d'affecter des règles communes de l'Union ou d'en altérer la portée. Le CEPD souligne qu'il est nécessaire de veiller à ce que la convention soit compatible avec le droit de l'Union, y compris avec la Charte, notamment les droits au respect de la vie privée et à la protection des données à caractère personnel, et avec l'article 16 du TFUE.

12. Le CEPD comprend que les services répressifs doivent pouvoir recueillir et obtenir des preuves électroniques rapidement et efficacement. Le CEPD rappelle toutefois que les Nations unies comptent de nombreux pays, lesquels disposent de systèmes juridiques extrêmement hétérogènes. Dans ce contexte, il estime qu'il existe un risque important que la convention puisse entraîner un affaiblissement de la protection des libertés et droits fondamentaux que le droit de l'Union garantit aux personnes physiques, notamment leurs droits à la protection des données et au respect de la vie privée.

13. Le CEPD souligne en outre qu'un instrument international similaire est déjà en vigueur, à savoir la convention sur la cybercriminalité et son deuxième protocole additionnel, récemment négocié et à présent ouvert à la signature.

14. Dans ce contexte, le CEPD tient à souligner que l'autorisation du Conseil à la Commission de participer aux négociations au nom de l'Union ne devrait pas être interprétée comme une obligation pour cette dernière de devenir partie à la convention en cas d'adoption, et notamment que **l'Union ne devrait pas chercher à être partie à une telle convention si elle risque de faire diminuer le niveau de protection des données que son droit garantit aux personnes physiques**.

15. Même si le CEPD reconnaît qu'il peut être impossible de transposer la terminologie et les définitions du droit de l'Union dans un accord avec de nombreux pays tiers, il insiste sur le fait que les garanties des particuliers doivent être claires et efficaces afin de pleinement respecter le droit de l'Union. Ces dernières années, la Cour de justice de l'Union européenne a de nouveau confirmé les principes relatifs à la protection des données, y compris le droit à un recours juridictionnel et les droits individuels des personnes. Ces principes s'avèrent d'autant plus importants que les données nécessaires aux enquêtes pénales sont sensibles.

16. Le présent avis vise à fournir des conseils constructifs et objectifs aux institutions de l'Union de façon à ce que le niveau de protection des données garanti par le droit de l'Union ne soit pas compromis. Il contient des recommandations supplémentaires sur les questions suivantes:

    - le rapport entre la convention et d'autres instruments;

    - le champ d'application de la convention;

    - les garanties concernant les transferts internationaux de données à caractère personnel;

[20] *Voir le considérant 3.*

- les dispositions finales de la convention (suspension, réexamen, établissement de relations).

17. Le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour fournir des conseils au cours des étapes ultérieures de ce processus.

3. Rapport avec d'autres instruments

18. Dans la recommandation[21], il est rappelé qu'il existe déjà un instrument international contraignant qui oblige ses parties à définir, dans leur droit national, certaines infractions pénales commises à l'encontre de réseaux électroniques ou au moyen de ceux-ci, qui prévoit des exigences minimales concernant les pouvoirs d'investigation disponibles dans le cadre d'une enquête pénale et qui encourage la coopération internationale entre les parties. Il s'agit de la **convention du Conseil de l'Europe sur la cybercriminalité (STE nº 185) (la «convention de Budapest»)**, qui est ouverte à la signature des États membres du Conseil de l'Europe et des États non membres qui ont participé à son élaboration ou à l'adhésion (sur invitation) des États non membres qui n'ont pas participé à son élaboration. À l'heure actuelle, 66 pays sont parties à la convention de Budapest, dont 26 États membres de l'Union[22] et d'autres pays tiers membres du Conseil de l'Europe comme l'Arménie, l'Azerbaïdjan ou la Turquie, ainsi que des pays non membres du Conseil de l'Europe, tels que l'Australie, le Canada, le Ghana, Israël, le Japon, le Maroc, le Paraguay, les Philippines, le Sénégal, le Sri Lanka, le Royaume de Tonga et les États-Unis[23]. En outre, le 17 novembre 2021, le Comité des Ministres du Conseil de l'Europe a adopté un deuxième protocole additionnel à la convention de Budapest, ouvert à la signature depuis le 12 mai 2022. Ce protocole vise à fournir des outils supplémentaires aux fins d'une coopération internationale, y compris aux fins d'une coopération en situation d'urgence[24].

19. Le CEPD **approuve le point 6 de l'annexe**, d'après lequel l'Union devrait parvenir à ce que la future convention des Nations unies soit «**compatible avec** les instruments internationaux **existants**, en particulier la convention de Budapest du Conseil de l'Europe de 2001 sur la cybercriminalité et ses protocoles, la convention des Nations unies de 2000 contre la criminalité transnationale organisée et ses protocoles, mais aussi avec les autres instruments internationaux et régionaux pertinents, et [...] les **complète**»[25] et à ce qu'elle «**évite toute incidence sur l'application de ces instruments** ou sur l'adhésion ultérieure de tout pays à ces derniers et, dans la mesure du possible, évite les redondances»[26].

---

[21] *Voir l'exposé des motifs, p. 1.*
[22] *Tous à l'exception de l'Irlande, qui a signé mais n'a pas ratifié la convention, et s'est néanmoins engagée à poursuivre son adhésion.*
[23] *Voir l'état des signatures et ratifications concernant la convention sur la cybercriminalité pour une liste exhaustive et actualisée des pays parties à la convention sur la cybercriminalité, disponible sur: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185*
[24] *Le 5 avril 2022, le Conseil de l'Union européenne a adopté une décision autorisant les États membres à signer, dans l'intérêt de l'Union, le deuxième protocole additionnel. Le même jour, il a également décidé de transmettre au Parlement, pour approbation, la décision autorisant les États membres à ratifier le protocole.*
[25] *Mise en évidence ajoutée.*
[26] *Mise en évidence ajoutée.*

20. Le CEPD **approuve** également **le point 17 de l'annexe**, d'après lequel l'Union devrait parvenir à ce que les «**mesures de coopération [...] [soient] compatibles avec ces conventions et avec les normes internationales en matière de droits de l'homme**», et le **point 23** de l'annexe, où il est clairement indiqué que l'Union devrait viser à parvenir à ce que la convention **préserve les instruments mondiaux et régionaux existants**.

21. Le CEPD **recommande** toutefois d'ajouter dans l'annexe que l'Union devrait parvenir à ce que **les futurs accords conclus avec des pays tiers s'appliquent en lieu et place de la convention s'ils garantissent des normes plus élevées en matière de protection des droits fondamentaux, notamment des droits au respect de la vie privée et à la protection des données**[27].

22. Enfin, le CEPD accueille favorablement et encourage vivement l'ajout, au point 23 de l'annexe, d'une «**clause de déconnexion**» destinée à garantir que le droit dérivé de l'Union continue de s'appliquer entre les États membres de l'Union, dans le but de préserver l'ordre juridique de cette dernière.

4. Champ d'application de la convention

4.1. Infractions pénales visées par la convention

23. Le CEPD approuve l'objectif consistant à **définir clairement et strictement** les infractions qui seraient visées par la convention, à savoir les «infractions qui ne peuvent être commises qu'au moyen de systèmes d'information» (**point 9** de l'annexe) et celles «qui peuvent être commises sans recours aux systèmes d'information mais qui, dans certaines circonstances, peuvent être facilitées par l'utilisation desdits systèmes, **mais uniquement lorsque la mobilisation de systèmes d'information modifie substantiellement les caractéristiques ou l'effet des infractions**» (point 10 de l'annexe) [mise en évidence ajoutée]. Il se dit également favorable à ce que les définitions doivent être «compatibles avec celles figurant dans les autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité, ainsi qu'avec les normes internationales en matière de droits de l'homme» (**point 11** de l'annexe).

24. Au **point 16 de l'annexe**, il est recommandé que la convention prévoie «*des mesures de coopération qui permettent aux autorités des différents États parties à l'instrument de coopérer efficacement aux fins d'enquêtes ou de procédures pénales concernant des infractions définies dans l'instrument* ***ou*** *de coopérer afin de conserver ou d'obtenir des preuves électroniques de* ***toute*** *infraction pénale dans le cadre d'une enquête ou d'une procédure pénales*» [mise en évidence ajoutée][28]. Le CEPD fait observer que les directives recommandées englobent les formes de coopération mise en place afin de conserver ou d'obtenir des preuves électroniques de toute infraction pénale dans le cadre d'une enquête ou d'une procédure pénales. Il considère que la limitation du champ d'application de la coopération

[27] *Voir par exemple la décision du Conseil autorisant l'ouverture de négociations avec le Japon en vue de modifier l'accord entre l'Union européenne et le Japon relatif à l'entraide judiciaire en matière pénale (12141/21) et la décision du Conseil autorisant l'ouverture de négociations en vue de conclure un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale (9114/19).*

[28] *Mise en évidence ajoutée.*

internationale au titre de la convention aux seules infractions pénales qui y sont définies constituerait une solide garantie de la nécessité et de la proportionnalité des solutions proposées, compte tenu des systèmes juridiques extrêmement hétérogènes des possibles futures parties à la convention. Par conséquent, le **CEPD estime que le champ d'application des futures dispositions en matière de coopération devrait lui aussi être limité aux infractions définies dans la convention**.

4.2. Exclusion de l'accès direct aux données et de la coopération directe avec les fournisseurs de services par les services répressifs

25. À ce stade précoce des négociations, le champ d'application de la convention reste flou, notamment en ce qui concerne les modalités de coopération.

26. Toutefois, comme il l'a déjà indiqué dans le cadre des négociations sur le deuxième protocole additionnel à la convention de Budapest[29], le CEPD considère que l'**accès direct transfrontière** des services répressifs de pays tiers aux données comme une mesure particulièrement intrusive et ayant donc davantage d'incidence sur les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. Par conséquent, il **estime que de telles dispositions ne devraient pas être introduites dans la convention et qu'il convient d'ajouter à l'annexe une directive à cette fin**.

27. Étant donné le nombre de pays susceptibles de devenir parties à la convention, lesquels disposent de systèmes juridiques extrêmement hétérogènes concernant le respect des droits et libertés fondamentaux, notamment des droits fondamentaux au respect de la vie privée et à la protection des données, le CEPD recommande également de s'opposer à toute tentative d'introduire dans la convention des dispositions régissant la coopération directe des autorités de pays tiers avec des fournisseurs de services soumis à la juridiction de l'Union. À cet égard, **il convient de préciser que le point 15 de l'annexe ne concerne que la coopération entre les services répressifs et les fournisseurs de services du même pays**, et non la coopération transfrontière entre les services répressifs et les fournisseurs de services d'un autre pays. Ce besoin de précision est d'autant plus grand que le point 19 de l'annexe indique que, dans le cadre de la convention, il convient de faire en sorte que les États membres de l'Union soient en mesure de se conformer aux exigences applicables aux transferts internationaux de données à caractère personnel au sens du RGPD, ce qui donne à entendre qu'une coopération directe entre les fournisseurs de services de l'Union et les autorités de pays tiers parties à la convention n'est en réalité pas exclue à ce stade.

[29] *Avis 3/2019 du CEPD relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité, points 18 et 19.*

5. Nécessité de garanties appropriées concernant les transferts internationaux de données et le respect des droits fondamentaux

28. Le CEPD rappelle que, en vertu de l'article 216, paragraphe 2, du TFUE, les accords internationaux conclus par l'Union «*lient les institutions de l'Union et les États membres*». En outre, selon la jurisprudence constante de la Cour de justice de l'Union européenne, les accords internationaux forment, à partir de leur entrée en vigueur, «*partie intégrante* [...] *de l'ordre juridique communautaire*»[30] et bénéficient de la primauté sur les actes de droit dérivé de l'Union[31].

29. Étant donné que la convention constituerait un instrument international qui permettrait à l'Union d'y devenir partie[32], le CEPD note que, conformément à la jurisprudence de la CJUE, «*les obligations qu'impose un accord international ne sauraient avoir pour effet de porter atteinte aux principes constitutionnels du traité CE, au nombre desquels figure le principe selon lequel tous les actes communautaires doivent respecter les droits fondamentaux, ce respect constituant une condition de leur légalité*»[33]. **Dès lors, il est essentiel de veiller à ce que les obligations découlant de la convention respectent pleinement le droit fondamental à la protection des données.**

30. Le CEPD approuve donc le **point 8 de l'annexe**, d'après lequel l'Union devrait parvenir à ce que les dispositions de la convention offrent la protection des droits de l'homme la plus élevée possible et à ce que les États membres de l'Union doivent être en mesure de se conformer au droit de l'Union, y compris aux droits fondamentaux, aux libertés et aux principes généraux du droit de l'Union tels qu'ils sont consacrés dans les traités européens et dans la Charte. Le CEPD se félicite également à cet égard de la référence claire au **principe de proportionnalité au point 13 de l'annexe**.

31. En outre, le CEPD souligne et **approuve le point 18 de l'annexe**, d'après lequel il conviendrait de parvenir à ce que les mesures de coopération soient soumises aux conditions prévues par le droit de la partie requise et prévoient des motifs de refus étendus de nature à garantir la protection des droits fondamentaux, dont le droit à la protection des données à caractère personnel, y compris dans le contexte des transferts de données à caractère personnel, et, s'il y a lieu, l'existence d'une double incrimination.

32. Le CEPD rappelle que, selon la jurisprudence de la CJUE, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services, «*prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées*»[34]. Lorsqu'il n'est pas possible de tirer de telles conclusions et que l'accès «ne saurait être qualifié d'ingérence "grave" dans les droits fondamentaux des personnes dont les données sont concernées», la Cour a en outre conclu que «*l'ingérence que comporterait*

---

[30] Arrêt de la Cour du 30 avril 1974, Haegemann/État belge, C-181/73, EU:C:1974:41, point 5.
[31] Arrêt de la Cour du 3 juin 2008, Intertanko e.a., C-308/06, EU:C:2008:312, point 42.
[32] Voir le point 25 de l'annexe.
[33] Arrêt de la Cour du 3 septembre 2008, Kadi et Al Barakaat International Foundation/Conseil et Commission, affaires jointes C-402/05 P et C-415/05 P, EU:C:2008:461, point 285.
[34] Arrêt de la Cour du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 54, voir également le point 56.

un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'"infractions pénales" en général, [...] *sans qu'il soit nécessaire que ces infractions soient qualifiées de "graves"*»[35].

33. Par conséquent, aux fins du respect de l'article 52, paragraphe 1, de la Charte, le CEPD estime que les catégories de données pour lesquelles la production et le transfert de données à caractère personnel pourraient être ordonnés doivent être proportionnelles aux types d'infractions en cause. **Plus précisément, il conviendrait de garantir que seule la criminalité grave est susceptible de justifier l'échange de données qui entraîne une ingérence grave dans les droits fondamentaux à la protection des données et au respect de la vie privée.**

34. Par ailleurs, le CEPD approuve le point 15 de l'annexe, d'après lequel l'Union devrait viser à parvenir à ce que les mesures procédurales visant à conserver ou à obtenir des preuves électroniques contiennent une définition claire et stricte du type d'informations visées. Il souligne l'importance de définir clairement et simplement les catégories de données dans la convention des Nations unies pour garantir à l'ensemble des acteurs concernés la sécurité juridique. **Le CEPD recommande de veiller à clairement définir les différentes catégories de données, ce qui contribuera à garantir la sécurité juridique.**

35. Le CEPD approuve le **point 19 de l'annexe** et **souligne son importance**. Celui-ci indique premièrement que **la convention devrait prévoir des conditions strictes et des garanties solides** afin que les États membres de l'Union puissent respecter et protéger les droits fondamentaux, les libertés et les principes généraux du droit de l'Union, tels qu'ils sont consacrés dans les traités européens et la Charte, y compris, en particulier, le principe de proportionnalité, le droit à un recours juridictionnel effectif, **le droit au respect de la vie privée, le droit à la protection des données à caractère personnel et des données de communications électroniques** lorsque ces données font l'objet d'un traitement, **y compris pour les transferts à des autorités situées dans des pays non membres de l'Union européenne**. Secondement, il dispose que, dans le cadre de la convention, il convient de faire en sorte que les États membres de l'Union **soient en mesure de se conformer aux exigences applicables aux transferts internationaux de données à caractère personnel au sens, notamment, de la directive (UE) 2016/680[36] et de la directive 2002/58/CE[37]**.

36. Dans le contexte particulier des transferts de données à caractère personnel à des fins répressives par les services de l'Union compétents en la matière, le CEPD rappelle que, en vertu de l'article 37 et du considérant 71 de la directive (UE) 2016/680, les transferts qui ne sont pas fondés sur une décision d'adéquation ne devraient être autorisés que lorsque des garanties appropriées ont été offertes dans un instrument juridiquement contraignant assurant la protection des données à caractère personnel, ou lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et estime, au vu de cette évaluation, qu'il existe des garanties appropriées. Ces instruments juridiquement contraignants pourraient être des accords bilatéraux juridiquement contraignants que les personnes concernées pourraient faire exécuter, qui respectent les

---

[35] *Idem, point 62. [Mise en évidence ajoutée].*
[36] *Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).*
[37] *Mise en évidence ajoutée.*

exigences en matière de protection des données et les droits des personnes concernées, y compris le droit à un recours administratif ou juridictionnel effectif. Le responsable du traitement devrait aussi pouvoir prendre en compte le fait que le transfert de données à caractère personnel sera soumis à des obligations de confidentialité et au principe de spécificité, ce qui garantit que les données ne seront pas traitées à des fins autres que celles pour lesquelles elles ont été transférées. En outre, le responsable du traitement devrait prendre en compte le fait que les données à caractère personnel ne seront pas utilisées pour demander, prononcer ou mettre à exécution une condamnation à la peine de mort ou toute forme de traitement cruel et inhumain. Le responsable du traitement devrait pouvoir exiger des garanties supplémentaires.

37. À cet égard, le CEPD **exprime de sérieux doutes quant à savoir si la future convention pourra servir de base autonome aux transferts de données à caractère personnel conformément au droit de l'Union** et recommande donc de garantir que les États membres sont en mesure d'exiger et d'imposer des garanties supplémentaires de sorte à n'autoriser les transferts dans le cadre de la convention que s'ils interviennent conformément au droit de l'Union, y compris le droit dérivé de l'Union.

38. Enfin, le CEPD tient à souligner en outre qu'il convient de définir précisément les autorités des pays tiers auxquelles les données seront transmises et qui traiteront ces données, afin de s'assurer qu'elles sont également compétentes au regard des finalités du transfert. Dès lors, en ce sens, le CEPD **recommande que la convention s'accompagne d'une liste exhaustive des autorités compétentes des pays destinataires auxquelles les données pourront être transmises ainsi que d'une brève description de leurs compétences. Cette préoccupation devrait également apparaître dans l'une des directives de l'annexe.**

6. Suspension, réexamen de la convention et établissement de liens conformément à la convention

39. Le CEPD approuve l'ajout d'une disposition spéciale **prévoyant la suspension** de la convention qui est inspirée, «lorsque cela est possible et approprié, des dispositions des autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité»[38]. Il **recommande** à cet égard de **préciser** que l'Union devrait viser à parvenir à ce qu'**un État contractant puisse**, au moment de la signature, de la ratification ou de l'adhésion, **déclarer qu'il n'exécutera aucune demande de transfert de données à caractère personnel à une autre partie si des indications[39] donnent à penser qu'un niveau essentiel de protection des données n'est plus garanti dans l'État demandeur.**

40. Le CEPD **recommande** également que l'annexe prévoie la demande d'introduction d'une clause définissant un **réexamen périodique obligatoire** du fonctionnement pratique de la convention. Afin de garantir un réexamen révélateur, celui-ci doit être prévu au plus tard cinq ans après l'entrée en vigueur de la convention, puis à intervalles réguliers. Il convient

[38] *Voir le point 24 de l'annexe.*
[39] *Comme pour la suspension demandée par le Comité des droits de l'homme des Nations unies.*

également de préciser la fréquence de ces réexamens complémentaires. Le contenu du réexamen devrait être précisé. Le réexamen devrait se concentrer non seulement sur la mise en œuvre de la convention, mais également sur l'évaluation de sa nécessité et de sa proportionnalité. Les équipes chargées du réexamen devraient se composer d'experts en protection des données, dont les représentants des autorités nationales de protection des données.

41. Enfin, compte tenu de l'extrême hétérogénéité des pays susceptibles d'être parties à la convention, le CEPD **recommande de prévoir dans le mandat que l'Union devrait viser à garantir que la convention ne produit aucun effet entre deux États contractants si l'un d'entre eux notifie** le fait que la ratification, l'acceptation, l'approbation ou l'adhésion d'un autre État contractant n'aura **pas** pour effet d'établir des relations entre ces deux États contractants en vertu de ladite convention[40].

7. Conclusions

42. Le CEPD **plaide en faveur** de l'adoption d'une décision du Conseil conférant un mandat clair à la Commission européenne pour participer, au nom de l'Union, aux négociations que les Nations unies mènent actuellement en vue de ladite convention. Cependant, il souligne que l'autorisation de participer aux négociations ne devrait pas obliger l'Union à devenir partie à la convention en cas d'adoption, et notamment que l'Union ne devrait pas chercher à être partie à une telle convention si le niveau de protection des données que son droit garantit aux personnes physiques devait diminuer.

43. Le CEPD approuve les points 6, 17 et 23 de l'annexe visant à préserver les instruments mondiaux et régionaux existants ainsi que les garanties prévues aux points 8, 9, 10, 11, 13, 18, 19 et 24 de l'annexe, et souligne leur importance.

44. À la lumière des considérations qui précèdent, le CEPD émet les recommandations exposées ci-après.

Concernant le rapport entre la convention et d'autres instruments

- Prévoir dans le mandat que l'Union devrait parvenir à ce que les futurs accords conclus avec des pays tiers s'appliquent en lieu et place de la convention s'ils garantissent des normes plus élevées en matière de protection des droits fondamentaux, notamment des droits au respect de la vie privée et à la protection des données.

Concernant le champ d'application de la convention

- Limiter les dispositions en matière coopération aux infractions pénales définies dans la convention.

[40] *Voir par exemple la convention de la Haye sur la reconnaissance et l'exécution des jugements étrangers en matière civile ou commerciale, la Haye, 2 juillet 2019, article 29.*

- Indiquer clairement dans le mandat que l'Union doit s'opposer à toute disposition relative à l'accès direct transfrontière aux données et à la coopération directe transfrontière avec des fournisseurs de services.

- Préciser que les directives visées au point 15 de l'annexe ne concernent pas la coopération transfrontière.

Concernant la nécessité de garanties appropriées et le respect des droits fondamentaux

- Indiquer clairement dans le mandat que l'Union devrait clairement définir les différentes catégories de données.

- Inclure une directive dans le mandat visant à parvenir à ce que la convention s'accompagne d'une liste exhaustive des autorités compétentes des pays destinataires auxquelles les données pourront être transmises ainsi que d'une brève description de leurs compétences.

Concernant les dispositions finales de la convention

- Préciser dans le mandat que l'Union devrait viser à parvenir à ce qu'un État contractant puisse, au moment de la signature, de la ratification ou de l'adhésion, déclarer qu'il n'exécutera aucune demande de transfert de données à caractère personnel à une autre partie si des indications donnent à penser qu'un niveau essentiel de protection des données n'est plus garanti dans l'État demandeur.

- Prévoir dans le mandat que l'Union devrait viser à parvenir à l'introduction d'une clause définissant un réexamen périodique obligatoire du fonctionnement pratique de la convention. Ce réexamen doit être prévu au plus tard cinq ans après l'entrée en vigueur de la convention, puis à intervalles réguliers. Il convient également de préciser la fréquence de ces réexamens complémentaires. Le contenu du réexamen devrait être précisé. Le réexamen devrait se concentrer non seulement sur la mise en œuvre de la convention, mais également sur l'évaluation de sa nécessité et de sa proportionnalité. Les équipes chargées du réexamen devraient se composer d'experts en protection des données, dont les représentants des autorités nationales de protection des données.

- Prévoir dans le mandat que l'Union devrait viser à garantir que la convention ne produit aucun effet entre deux États contractants si l'un d'entre eux notifie le fait que la ratification, l'acceptation, l'approbation ou l'adhésion d'un autre État contractant n'aura pas pour effet d'établir des relations entre ces deux États contractants en vertu de ladite convention

45. Enfin, le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour fournir des conseils au cours des étapes ultérieures de ce processus. Les observations présentées dans le présent avis sont sans préjudice des observations supplémentaires que le CEPD pourrait formuler ultérieurement, notamment si de nouvelles questions devaient être soulevées et abordées à la lumière d'informations complémentaires. Le CEPD s'attend à être consulté à propos des dispositions du projet de convention avant que celui-ci ne soit finalisé.

Bruxelles, le 18 mai 2022

(signature électronique)
Wojciech Rafał Wiewiórowski